Genuine Route Identifier (GRI) scheme for USOR to Restrict Worm hole Attack in MANET

Maharani.R[*1],Kanagaraju.P[*2]
[1]*PG Scholar of Computer Science, K.S.Rangasamy College of Technology, Tiruchengode, India.*
Email: maharanicse@gmail.com, Mobile No: +91 9842045954.
[2]*Assistant professor (Academic), K S Rangasamy College of Technology, Tiruchengode, India.*
Email:kanagarajup@gmail.com

***Abstract*--Privacy protection in Ad Hoc network becomes key issue in privacy-preserving routing. Earlier works on privacy preserving routing did not address unlinkability or unobservability property due to data packets and control packets are linkable and distinguishable. Existing work presents privacy requirements with Unobservable Secure On-Demand Routing (USOR) scheme which offers complete unlinkability and content unobservability for all types of packets. USOR used combination of group signature and ID-based encryption for secured route discovery. But it unable to detect the propagation of wrong topology information in illusion channel due to the wormhole attack which disrupt the route reply and topology control messages. To restrict Worm hole Attack in MANET, Proposal work develops an efficient Genuine Route Identifier (GRI) scheme. GRI scheme protects the worm hole in capturing topology information and restricts advertising to other colluding nodes. Each route reply is verified with route identifier based on its past history and genuine routes are identified along with false route as well. False routes are broadcasted to other nodes for genuine route verification. The simulations are carried out with ns2 on a developed GRI scheme that exhibits our proposed scheme has comparable performance to existing Privacy protection schemes USOR and MASK**.

***Keywords*--Privacy protection, Genuine Route, Worm hole, Security, Anonymity.**

I. INTRODUCTION

In today's development, concerns about the security of user's privacy characterize one of the main reasons that bound the extensive dispersal of mobile services. Even though the requirement of privacy solutions for mobile users rises, obtainable solutions are only palliative and fragile in mobile situations. Privacy solutions in fact chiefly concentrate on protecting the users against services that gather the user's personal data for service provisioning. On the other hand, the arrival of cellular (and in general hybrid) networks have prepared the problem of protecting the users' privacy worse: users must also be secluded from the prying eyes of mobile peers and mobile network operators. Privacy protection of mobile ad hoc networks (MANETs) is more difficult than that of wired networks because of the open nature and mobility of wireless media. Offering privacy protection for ad hoc networks with low-power wireless devices and low-bandwidth network link is a very demanding task. Privacy protection in routing of MANET has concerned a lot of investigate efforts. Total unlinkability and unobservability are not assured due to incomplete content protection. Earlier works fail to defend all content of packets from attackers, consequently that the attacker can get information like packet type and sequence number etc. Existing work used USOR scheme that attains content unobservability by using anonymous key establishment based on group signature. In USOR each node only has to obtain a group signature signing key and an ID-based private key from an offline key server or by a key management scheme. But it incapable to identify worm hole attacks. As a result of the worm hole attacks illusion channel propagate wrong topology information. Wormhole attacks disrupt the route reply and topology control messages and advertise the abnormal routes to the colluding nodes. To surmount these problems, proposal in this paper presents a scheme to resist wormhole attack to preserve privacy route information in ad hoc network. Genuine route identifier scheme is presented to increase the routing data throughput and reduce the routing delay on route discovery mechanism.

II. LITERATURE REVIEW

Several routing schemes have been introduced for ad hoc networks in recent years, and they provide different level of privacy protection at different cost. An analysis framework has been developed in [1] that allows quick, back-of-the envelope calculation to assess the effectiveness of batching strategies in countering flow correlation attacks. Peer-to-peer privacy of both payload and control messages using a cryptographically lightweight protocol relying solely on symmetric cryptography for its operation was provided in [2]. Research in [3] introduced embedded authenticated key exchange mechanisms for

MANETs which is anonymous secure routing protocol, ASRPAKE. Anonymity is an important part of the overall security architecture for mobile ad hoc networks as it allows users to hide their activities. This enables private communications between users while making it harder for adversaries to focus their attacks [4]. Unique anonymity threats in mobile ad hoc environments were analyzed by ANODR in [5].Pairing-based anonymous on-demand routing protocol, called MASK, [6] is to prevent malicious traffic analysis by passive adversaries. The ALARM framework is framed which supports anonymous location-based routing in certain types of suspicious MANETS. ALARM relies on group signatures to construct one-time pseudonyms used to identify nodes at certain locations [7].Lightweight and non path-based mutual anonymity protocol is suggested for unstructured P2P (Peer-to-peer) systems, Rumor Riding (RR) [8]. A group signature scheme based on the Strong Diffie-Hellman (SDH) and Linear assumptions is framed in [9].

Identity-based encryption was to simplify certificate management in e-mail systems which can use three keys namely Public key, Private Key and Master key [10]. Information-theoretic metric is based on the idea of anonymity probability distributions and use the metric to compare the pool mix to more traditional mixes [11].Decentralized protocol is found for limiting the corruptive influences of sybil attacks, by bounding both the number and size of sybil groups [12]. Elliptical Curve Cryptography (ECC) is used for the software implementation of the on workstations of the NIST. It has got good commercial acceptance and it is more efficient and secure [13].

III.AN UNOBSERVABLE SECURE ON-DEMAND ROUTING PROTOCOL

Privacy-preserving routing is crucial for some ad hoc networks that require stronger privacy protection. A number of schemes have been proposed to protect privacy in ad hoc networks. One of such schemes is USOR. In this scheme, both control packets and data packets look random and indistinguishable from dummy packets for outside adversaries. Only valid nodes can distinguish routing packets and data packets from dummy traffic with inexpensive symmetric decryption. But it can not identify wormhole attacks. When this attack targets specifically routing control packets, the nodes that are close to the attackers are shielded from any alternative routes with more than one or two hops to the remote location. All routes are thus directed to the wormhole established by the attackers. To identify wormhole attacks, this work develops Genuine route identifier scheme (GRI scheme). GRI is designed mainly for the purpose of maintaining security of the users and the messages they send. It protects the worm hole in capturing topology information and limits advertising to other colluding nodes. Each route reply is confirmed with route identifier based on its precedent history and authentic routes are recognized along with fake route as well. Fake routes are transmited to other nodes for authentic route confirmation. Genuine route identifier scheme is presented to increase the routing data throughput and reduce the routing delay on route discovery mechanism. This process is illustrated in fig.1The Unobservability Secure On-demand Routing protocol has five phases as follows:

- Ad Hoc Network Communication
- Worm Hole Attack Initiation
- Unobservable Secured Routing
- Restriction of Colluding Node and Advertising
- Genuine Route Identifier (GRI)

A. AdHoc Network Communication:

A mobile ad-hoc network (MANET) is a self-configuring infrastructureless network of mobile devices connected by wireless. Mobile nodes are distributed and also node parameters are initialized in MANETs. Source and destination are identified correctly. They have their own pair identification. The route discovery phase is an important phase in Ad Hoc networks. This process involves the steps namely: Broadcasting the route request, acknowledging the route reply and Identifying the best required path.

Data forwarding is done as follows. First the source receives the route reply with the cache route included in it. Source node sends the data packets to the destination. The packet header contains the entire route. The intermediate node uses the source node and they forward the packets to next node. Forwarding continues till the destination is reached. MANET network can be disturbed by several attacks in transmitting/ receiving data. A particularly rigorous attack on routing protocols in MANETs is wormhole attack in which two or more colluding attackers record packets at one location, and channel them to some other location for a replay at that secluded location.

B. WormHole Attack Initiation

Wormhole attacks are one of most easy to deploy for such an adversary and can cause great damage to the network. Initialization of wormhole attack is made on the mobile nodes. Two colluding nodes are connected through a tunnel. An illusive neighbor in the network has been generated. These illusive neighbors mislead the route request packets. Because of this the malicious nodes get the route request packets and they extract the topology information. The colliding node is propagated through tunnels. This warm attack process is replayed in the other nodes as well. The malicious mobile nodes initiating wormhole attacks in ad hoc network regions has been marked.

C. Unobservable Secured Routing

The privacy needs are evaluated using the Unobservable Secure Routing Scheme. This provides complete unlinkability across the wireless networks. This contributes the content unobservability for all kinds of They develop a group signature

The key establishment protocol is designed following the principal of KAM.

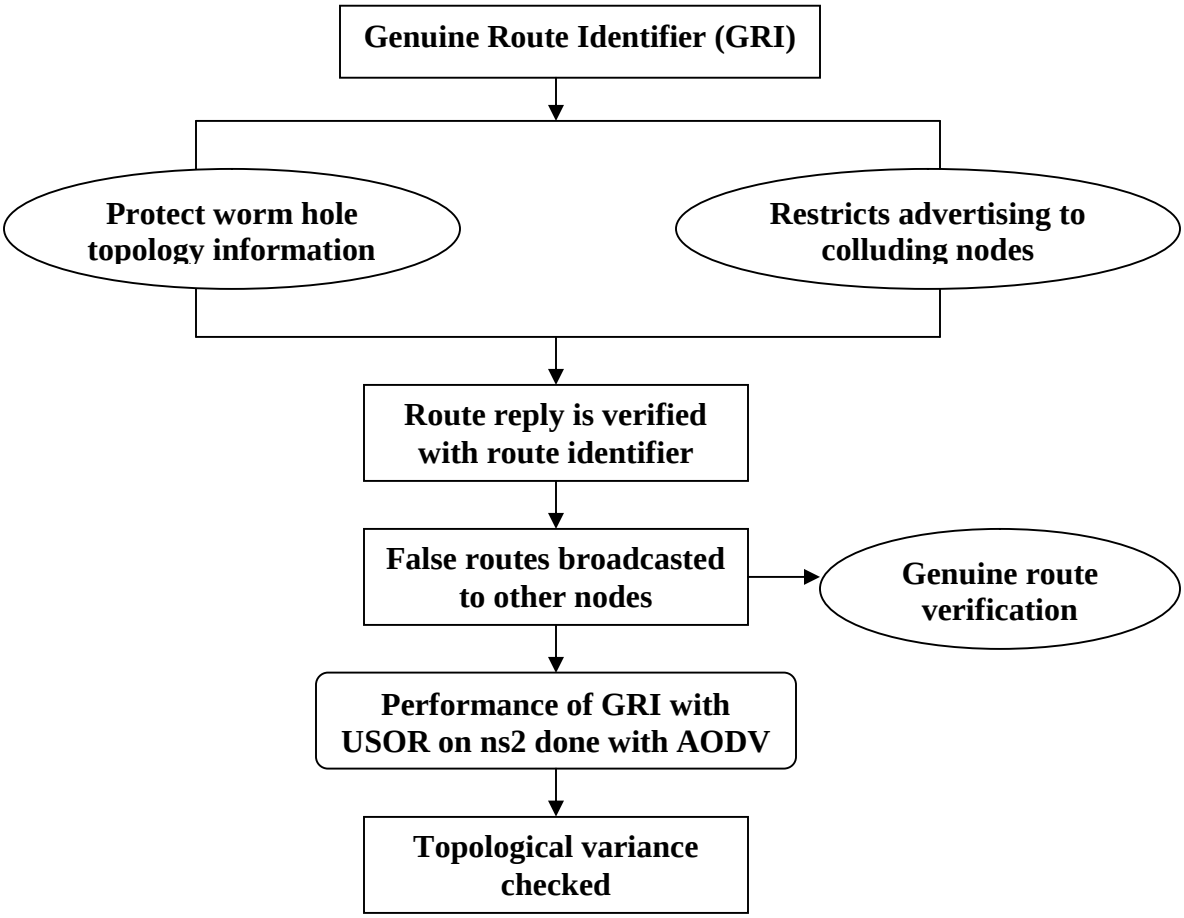

Fig 1. Genuine Route Identifier (GRI) scheme for UOSR to Restrict Worm hole Attack in MANET

Route discovery is done with ID-based encryption and that Utilize anonymous key for route id crypting. Secured routing protect user privacy against inside and outside attackers. Though Unobservable Secure On-Demand Routing offers complete unlinkability and content unobservability for all types of packets, it unable to detect the propagation of wrong topology information in illusion channel due to the wormhole attack, disrupts the route reply and topology control messages. Unobsevable routing scheme comprises of two phases anonymous key establishment as the first phase and route discovery process as a second phase.

D. Restriction of Colluding Node and Advertising

Mobile nodes which monitors and other nodes which forward the packets may come across a collision. The intermediate node packet which is forwarded to other node causes collision. Wormhole attack uses the collision to form illusive routes. These illusive routes are generated by forming channel between collusion nodes. This channel has been propagated to other collision nodes too. To find the previous path of the route used, we have to monitor and check the channel path of the network. Channel with unused history with

improper route id are discarded. This is the important part of advertising and so we have to be alert and cautious. Hearing of route reply path with authentic route id and usage history is ensured for data forwarding. Compromised nodes have direct

communication links. Authentic keys are issued to communicating neighboring nodes. Even though compromised nodes collude and share their keys, Malicious adversary unable to access all the keys of the network

E. Genuine Route Identifier (GRI)

The first step for the genuine route identification is finding out the route reply for the source nodes. We have to check the route path of a mobile node by checking out the route path of the previous route path history of the mobile node. Ensure the topological information is authenticated with the varied conditions of the network. We have to evaluate the rate of route path which is previously used and also the data forwarding the status. The routes which has, generally, high forwarding rate are identified as genuine routes. Routes which has poor forwarding rate are termed as false or fake routes. This forwarding rate depends on the heuristic threshold. False routes are broadcasted to other nodes for warning. Therefore, all the nodes are alert of these false routes. By using GRI scheme Genuine Route is identified easily.

IV. PERFORMANCE EVALUATION ON UNOBSERVABLE SECURE ON-DEMAND ROUTING

In this section, we use NS2 simulation to evaluate Genuine Route Identifier (GRI) scheme and compare it with other routing protocols. Our evaluation concerns the authority from both the processing time needed to carry out the security operations and the increased sizes of routing control packets on network performance. The simulation is performed in NS2 simulator and IEEE 802.11 is exploited as the MAC layer in our experiments. The radio employs the two-ray ground reflection propagation model and the channel capacity is 2Mbps. The network field is 1100m * 1100m with 50 nodes initially uniformly distributed and the transmission range is 250m. Random Way Point (RWP) model is exploited to simulate node mobility. In our NS2 simulation, the mobility is controlled in such a way that minimum and maximum speeds are forever the similar. Mobility is increased from 0 to 10 m/sec in various runs. CBR sessions are used to produce network data traffic. For every session, data packets of 512 bytes are produced in a rate of 4 packets per second. The source and destination pairs are selected randomly from all the nodes.

We evaluate the performance of GRI in terms of the overall network performance (delivery metric) and the influence from processing delay (delay metric) and packet size (overhead metric). We employ the following metrics: packet delivery ratio, packet latency, and Normalized Control Bytes per data packet delivered.

V. EXPERIMENTAL RESULTS AND DISCUSSION

In this section, we give simulation results for increasing mobility from 0 to 10 m/s. Genuine Route Identifier (GRI) scheme is evaluated with different performance metrics and compares it with other routing protocols such as USOR and MASK. By comparing GRI with USOR and MASK, the simulation results show that GRI not only has satisfactory performance, but also achieves stronger privacy protection than USOR, MASK.

Table 1: Packet Delivery ratio (%)

Mobility(m/s)	**Packet Delivery ratio(%)**		
	GRI	**USOR**	**MASK**
2	94.57	84.25	79.03
4	93.81	81.33	74.92
6	95.02	70.85	59.65
8	92.12	66.39	57.48
10	89.98	64.38	51.74

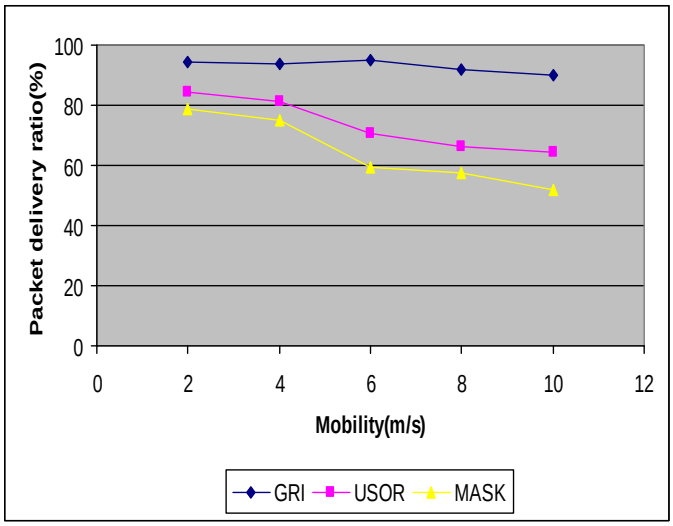

Figure 5.1: Packet Delivery ratio (%)

Figure 5.1 shows the comparison result of packet delivery ratio. GRI indicates the best performance possible on this metric, because it used efficient security mechanism when exchanging routing packets, effectively accelerating the route discovery process. USOR and MASK experience moderate delivery ratio degression. The reasons are that the two protocols need more security at the destination nodes. In a mobile environment, excessive delay in route discovery process makes it harder to establish and maintain routes. All the curves show a more or less yet steady descendant when mobility increases. This is natural as increasing mobility will cause more packet losses. Figure 5.1 shows better delivery ratio performance of GRI than existing USOR and MASK. GRI achieves 10% to 38% higher delivery ratio result.

Table 2: Latency

Mobility(m/s)	Latency(ms)		
	GRI	USOR	MASK
2	12.324	35.47	56.02
4	13.455	96.38	97.238
6	63.356	107.05	103.84
8	74.23	178.9	185.93
10	81.56	193.95	219.85

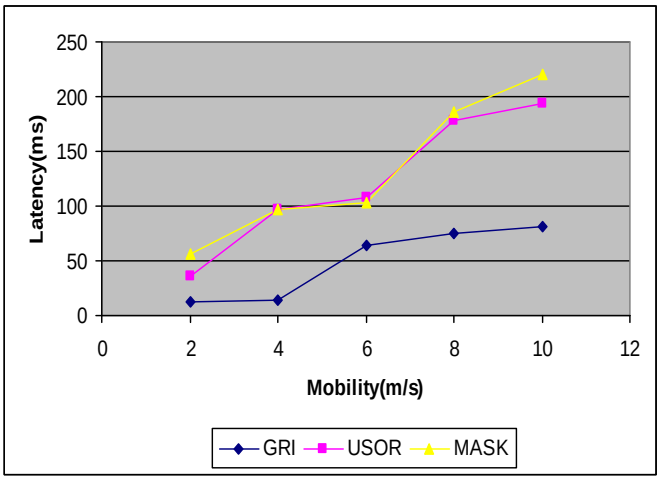

Figure 5.2: End-to-end latency

Figure 5.2 demonstrates the data packet latency. When there is little mobility, all protocols display small data packet latency, because once a route is established, a stable network allows a longer average route lifetime. When mobility increases, data packet latency increases accordingly. Because of the security overhead, USOR and MASK show significant longer end-to-end latency. Figure 5.2 shows better performance of GRI in terms of latency than existing MASK and USOR. GRI achieves 12% to 29% less end-to-end latency when compared with existing schemes.

Table 3: Normalized Control Bytes

Mobility(m/s)	Normalized Control Bytes		
	GRI	USOR	MASK
2	0.23	0.36	0.78
4	0.34	1.75	2.83
6	0.52	3.78	5.31
8	1.27	4.94	8.93
10	1.33	7.82	9.22

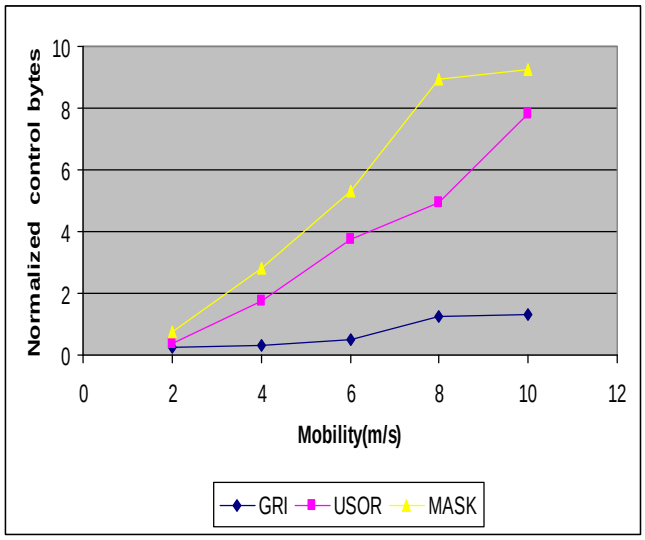

Figure 5.3: Normalized control bytes

Figure 5.3 compares the normalized control overhead in terms of bytes. MASK and USOR generate the most normalized control bytes, GRI less. In addition, USOR and MASK are low in the number of successfully delivered packets and USOR has closer values with MASK. When mobility increases, Normalized control bytes increases accordingly. Figure 5.3 shows GRI has less Normalized control bytes than existing USOR and MASK. GRI achieves 14% to 32% less Normalized control bytes when compared with existing schemes.

VI. CONCLUSION

In this paper, we presented the privacy-preserving routing scheme for mobile ad hoc networks. We have developed an efficient Genuine Route Identifier (GRI) scheme to restrict Worm hole Attack in MANET. The design of GRI scheme attempts to detect situations which might create the poor performance characteristic of an enduring wormhole attack. By using proposed GRI scheme, each route reply has been verified with route identifier based on its past history and genuine routes have been identified along with false route as well. Performance of Genuine Route Identifier (GRI) scheme is evaluated by using NS2 simulator that shows GRI scheme attained better performance in terms of packet delivery ratio (10% to 38% higher), latency (12% to 29% less) and normalized control bytes(14% to 32% less) when compared with existing schemes USOR and MASK.

REFERENCES

[1] Y. Zhu, X. Fu, B. Graham, R. Bettati, and W. Zhao, "On flow correlation attacks and countermeasures in mix networks," in PET04, LNCS 3424, 2004, pp. 207–225.
[2] J. Kong and X. Hong, "ANODR: aonymous on demand routing with untraceable routes for mobile ad-hoc networks," in Proc. ACM MOBIHOC' 03, pp. 291–302.
[3] B. Zhu, Z. Wan, F. Bao, R. H. Deng, and M. KankanHalli, "Anonymous secure routing in mobile ad-hoc networks," in Proc. 2004 IEEE Conference on Local Computer Networks, pp. 102–108.
[4] S. Seys and B. Preneel, "ARM: anonymous routing protocol for mobile ad hoc networks," in Proc. 2006 IEEE International Conference on Advanced Information Networking and Applications, pp. 133–137.
[5] D. Sy, R. Chen, and L. Bao, "ODAR: on-demand anonymous routing in ad hoc networks," in 2006 IEEE Conference on Mobile Ad-hoc and Sensor Systems.
[6] Y. Zhang, W. Liu, and W. Lou, "Anonymous communications in mobile ad hoc networks," in 2005 IEEE INFOCOM.
[7] K. E. Defrawy and G. Tsudik, "ALARM: anonymous location-aided routing in suspicious MANETs," IEEE Trans. Mobile Comput., vol. 10, no. 9, pp. 1345–1358, 2011.
[8] Y. Liu, J. Han, and J. Wang, "Rumor riding: anonymizing unstructured peer-to-peer systems," IEEE Trans. Parallel Distrib. Syst., vol. 22, no. 3, pp. 464–475, 2011.
[9] D. Boneh, X. Boyen, and H. Shacham, "Short group signatures," in Advances in Cryptology–Crypto'04, Lecture Notes in Computer Science, vol. 3152, 2004, pp. 41–55.
[10] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," in Advances in Cryptology–Crypto'01, Lecture Notes in Computer Science, vol. 2139, 2001, pp. 213–229.
[11] A. Serjantov and G. Danezis, "Towards an information theoretic metric for anonymity," in Privacy Enhancing Technologies, 2002, pp. 41–53.
[12] H. Yu, M. Kaminsky, P. B. Gibbons, and A. Flaxman, "Sybilguard: defending against sybil attacks via social networks," in Proc. 2006 SIGCOMM, pp. 267–278.

[13] M. Brown, D. Hankerson, J. L´opez, and A. Menezes, "Software implementation of the NIST elliptic curves over prime fields," in Topics in Cryptology – CT-RSA 2001, LNCS, vol. 2020, 2001, pp. 250–265.